SPECIAL ISSUE

Kenya Gazette Supplement No. 125 (National Assembly Bills No. 61)

REPUBLIC OF KENYA

KENYA GAZETTE SUPPLEMENT

NATIONAL ASSEMBLY BILLS, 2019

NAIROBI, 24th July, 2019

CONTENT

Bill for Introduction into the National Assembly—

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI

THE KENYA INFORMATION AND COMMUNICATIONS (AMENDMENT) BILL, 2019

A Bill for

AN ACT of Parliament to amend the Kenya Information and Communications Act.

ENACTED by the Parliament of Kenya, as follows—

PART I—PRELIMINARY

Short title.

1. This Act may be cited as the Kenya Information and Communications (Amendment) Act, 2019.

Amendment of section 2 of Act No. 2 of 1998.

2. The Kenya Information and Communications Act (hereinafter referred to as "the Principal Act") is amended in section 2 by inserting the following new definitions in the proper alphabetical sequence—

"blogger"means any person who is registered as such by the Commission under section 84D;

"blogging" means collecting, writing, editing and presenting of news or news articles in social media platforms or in the internet;

"social media platforms" includes online publishing and discussion, media sharing, blogging, social networking, document and data sharing repositories, social media applications, social bookmarking and widgets;

"widgets" means an application, or a component of an interface, that enables a user to access a service.

New Part.

3. The Principal Act is amended by inserting the following new Part immediately after Part VIA.

PART VIAA—REGULATION OF SOCIAL MEDIA

Licensing of Social media platforms.

84IA. (1) The Commission may on application in a prescribed manner and upon payment of a prescribed fee, grant a licence authorising any person to establish a social media platform for purposes of communication.

(2) A licence granted under this Part may be issued by an applicant subject to

such terms and conditions as the Commission may think fit, and may include—

(a) the establishment of a physical office in the country;

(b) the registration of all users of the social media platform using legal documents;

(c) a requirement that the licensee shall keep all the data of the users of it's platform and shall submit the same to the Commission when required; and

(d) a requirement that the licensee shall carry out due diligence to ensure that all its users, if natural persons are of age of majority.

(3) The Commission may revoke a licence granted under this section where the licensee is in breach of its terms and conditions provided under subsection (2).

Sharing of information.

84IB. A licensee may collect, use, preserve, and share information of its user where it is reasonably necessary to respond to a legal process.

Social media users responsibility.

84IC. (1) A social media user shall ensure that any content published, written or shared through the social media platform—

(a) does not degrade or intimidate a recipient of the content;

(b) is not prejudicial against a person or group of people based on their race, gender, ethnicity, nationality, religion, political affiliation, language, ability or appearance; and

(c) is fair, accurate and unbiased.

(2) Where a social media platform is created for a group of persons, it shall be the responsibility of the group administrator to—

(a) notify the licensee of the social media platform of his or her intentions to form a group platform;

(b) approve the members of the group;

(c) approve the content to be published in the platform; and

(d) control undesirable content and discussion.

(3) Any person who contravenes the provision of this section commits an offence and shall be liable upon conviction to a fine not exceeding two hundred thousand shillings, or to an imprisonment of a term not exceeding one year.

Registration of bloggers.

84ID.(1) The Commission may upon application in a prescribed manner and subject to such conditions as it may deem necessary, grant a licence authorizing any person to blogs.

(2) The Commission shall keep a register of bloggers in a prescribed manner.

(3) Any person who blogs without a licence is guilty of an offence.

(4) Any person who contravenes the provision of this section commits an offence and shall be liable upon conviction to a fine not exceeding five hundred thousand shillings, or to an imprisonment of a term not exceeding two years.

Bloggers code of conduct.

84IE. (1) The Commission shall develop a bloggers code of conduct.

MEMORANDUM OF OBJECTS AND REASONS

Statement of Objects and Reasons for the Bill

The objective of this Bill is to amend the Kenya Information and Communications Act to provide for regulation of use of social media platforms.

Clause 1 of the Bill provides for the short title of the Bill.

Clause 2 provides for new definitions for clarity purposes.

Clause 3 seeks to introduce a new Part to the Act on regulation of social media platforms. The new part will introduce new sections to the Act on licensing of social media platforms, sharing of information by a licensed person, creates obligations to social media users, registration of bloggers and seeks to give responsibility to the Communications Authority to develop a bloggers code of conduct in consultation with bloggers.

Statement on the delegation of legislative powers and limitation of fundamental rights and freedoms

The Bill does not delegate any legislative powers, and it does not limit fundaments rights and freedoms.

Statement on how the Bill does concerns county governments

The Bill does not concern county governments in terms of Articles 110(1)(a) of the Constitution.

Statements that the Bill is not a money Bill within the meaning of Article 114 of the Constitution

The Bill is not a money Bill for the purposes of Article 114 of the Constitution, the enactment of this Bill will not occasion additional expenditure of public funds.

M. M. INJENDI,
Member of Parliament.

Sections to be amended by the Bill

2. Interpretation

(1) In this Act unless, the context otherwise requires—

"access" in relation to any computer system", means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system;

"act of vandalism" means any willful, negligent, reckless or malicious act of stealing, destroying, damaging or breaking into telecommunications apparatus, lines, installations, hardware, software or plant used for telecommunication services and systems;

"advanced electronic signature" means an electronic signature which meets all the following requirements—

(a) is uniquely linked to the signatory;

(b) is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change to the data is detectable;

"agreement" includes decisions or practices;

"Authority" means the Communications Authority of Kenya established under section 3;

"Board" means the Board of Directors constituted under section 6;

"broadcaster" means any legal or natural person who composes or packages or distributes television or radio programme services for reception by the public or sections of the public or subscribers to such a service, irrespective of technology used;

"broadcasting" means unidirectional conveyance of sounds or television programmes, whether encrypted or not by radio or other means of telecommunications, for reception by the public;

"broadcasting service" means any service which consists of the broadcasting of television or sound broadcasting programs to the public, sections of the public or subscribers to such a service;

"broadcasting signal distribution" means the process whereby the output signal of a broadcasting service is taken from the point of origin, being the point where such signal is made available in its final content format, from where it is conveyed to any broadcast target area by means of a telecommunication process and includes multi-channel distribution;

"Cabinet Secretary" means the Cabinet Secretary for the time being responsible for information, communication and technology;

"certificate" means a record which is issued by a certification service provider for the purpose of supporting a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair; identifies the certification service provider issuing it; names or identifies the person to whom it is issued; contains the public key of the person to whom it is issued; and is signed by a responsible officer of the certification service provider issuing it;

"certification service provider" means a person who has been granted a licence to issue a digital signature certificate;

"Commission" means the Communications Authority of Kenya;

"community" includes a geographically founded community or any group of persons or sector of the public having a specific, ascertainable common interest;

"community broadcasting service" means a broadcasting service which meets all the following requirements—

(a) is fully controlled by a non-profit entity and carried on for non-profitable purposes;

(b) serves a particular community;

(c) encourages members of the community served by it or persons associated with or promoting the interests of such community to participate in the selection and provision of programmes to be broadcast in the course of such broadcasting service; and

(d) may be funded by donations, grants, sponsorships or membership fees, or by any combination of the aforementioned;

"computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, software and communication facilities which are connected or related as a system or network;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device or collection of devices including input and output devices but excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions and

data that perform logic, arithmetic, data storage, data retrieval, communication control and other functions;

"country code top-level domain" means top-level domain .ke used and reserved for Kenya;

"courier services" means any specialised service for the collection, despatch, conveyance, handling and delivery of postal articles;

"customs law" means any law relating to the collection of customs duties or transfer tax;

"cyber security"means the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment;

"data" means information recorded in a format in which it can be processed by equipment operating automatically in response to instructions given for that purpose, and includes representations of facts, information and concepts held in any removable storage medium;

"Director-General" means the Director-General of the Commission appointed under section 6;

"document of title" means a formal document that is considered sufficient proof that the person who possesses it is entitled to receive, hold, and dispose of the instrument and the goods that it covers;

"dominant telecommunications service provider" means a licensee determined to be a dominant telecommunications service provider pursuant to the criteria set out in sections 4 and 23 of the Competitions Act, 2014;

"e-Government services" means public services provided electronically by a Ministry or Government department, local authority, or any body established by or under any law or controlled or funded by the Government;

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities;

"electronic form" with reference to information, means any information generated, sent, received or stored in magnetic, optical, computer memory, microfilm or similar device;

"electronic Gazette" means the Kenya Gazette published in electronic form;

"electronic record" means a record generated in digital form by an information system, which can be transmitted within an information

system or from one information system to another and stored in an information system or other medium;

"electronic signature" means data in electronic form affixed to or logically associated with other electronic data which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;

"encryption" means a method transforming signals in a systematic way so that the signal would be unintelligible without a suitable receiving apparatus;

"equipment" includes any appliance, apparatus or accessory used or intended to be used for communication services;

"financial year" means a financial year within the meaning of section 18;

"former Commission" means the Communications Commission of Kenya immediately existing before the commencement of this Act;

"franking machine" means a machine for the purpose of making impressions on postal articles to denote pre-payment of postage and includes any meter or meters and any franking or date-stamping die incidental thereto;

"free-to-air service" means a service which is broadcast without encryption and capable of being received by conventional broadcasting receiving apparatus;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"Fund" means the Universal Service Fund established by section 84J of this Act;

"information and communication technologies" means technologies employed in collecting, storing, using or sending out information and include those involving the use of computers or any telecommunication system;

"installation or plant used for posts" includes all buildings, lands, structures, machinery, equipment, boxes and receptacles used or intended for use in connection with the transmission of postal articles by post;

"intercept" in relation to a function of a computer, includes listening to, or recording a function of a computer, or acquiring the substance, its meaning or purport of such function;

"Kenyan programme" means sounds or vision or a combination of both whose content comply with the classification of local content as may be required by the Commission from time to time;

"letter" means any written or printed communication conveying from one person to another particular information upon matters personal to such persons or information upon which it is intended that the recipient should reply, act or refrain from acting, but does not include any written or printed communication which is a newspaper or a periodical accompanied by any other communication;

"licence" means any licence issued under this Act;

"mail bag" means any bag, container, envelope or covering in which postal articles are conveyed;

"market" means a market in Kenya or a substantial part of Kenya and refers to the range of reasonable possibilities for substitution in supply or demand between particular kinds of goods or services and between suppliers or acquirers, or potential suppliers or acquirers, of those goods or services;

"media" means broadcast, electronic and other types of media but does not include print and book publishing;

"Media Council" means the Media Council of Kenya established under the Media Council Act;

"Minister" means Cabinet Secretary;

"modification" means a modification of the contents of any computer system by the operation of any function of that computer system or any other computer system as a result of which—

(a) any program or data held in the computer system is altered or erased;

(b) any program or data is added to its contents; or

(c) any act occurs which impairs the normal operation of the computer system;

"parcel" means a postal article which is posted at the office of a licensee as a parcel or is received at another office:

Provided that the said parcel is not smaller than the minimum size or heavier than the maximum weight prescribed;

"password" means any data by which a computer service or a computer system is capable of being obtained or used;

"possession", "be in possession of" and "have in possession" have the meanings assigned to such expressions in section 4 of the Penal Code, (Cap. 63);

"post"—

(a) when used with reference to telecommunication includes any pole, standard, stay, strut or other above-ground contrivance for

installing, carrying, supporting or suspending a telecommunication line; and

(b) when used with reference to the transmission of postal articles by post, means any system for the collection, dispatch, conveyance, handling and delivery of postal articles;

"post office" means any building, house, room, receptacle, vessel, vehicle or place where postal articles are received, delivered, sorted, made up or despatched;

"postage" means the fee chargeable for the transmission by post of postal articles;

"postage stamp" means any label or stamp for denoting any postage or other sum payable in respect of a postal article, and includes an adhesive postage stamp or a stamp printed, impressed or otherwise indicated on a postal article, whether issued by the Government of Kenya or any other country;

"postal article" means any article or thing transmissible by post, including but not limited to letters, aerogrammes, postcards and parcels but does include such article or thing as the Commission determines not to be transmissible by post;

"postal service" means any service by post;

"postcard" means a card recognised as a postcard in accordance with the terms of the Convention regulating the affairs of the Universal Postal Union;

"posting box" includes any pillar box, wall box, any other box or receptacle provided by or under the authority of the public postal licensee for the purpose of receiving postal articles for transmission by or under the authority of the public postal licensee;

"private broadcaster" means a person licensed by the Commission under this Act to provide commercial broadcast services;

"private letter box/bag" means any receptacle whether identified by a distinctive number or not rented to a person for the receipt of postal articles and capable of being used whether the person or company renting it has his business premises open or not;

"programme" means sound, vision or a combination of both, intended to inform, educate or entertain, but does not include text or data;

"public broadcaster" means the Kenya Broadcasting Corporation established by the Kenya Broadcasting Corporation Act (Cap. 221);

"public broadcasting services" means broadcasting services of the public broadcaster;

"public postal licensee" means the Postal Corporation of Kenya established under the Postal Corporation of Kenya Act, 1998 (No. 3 of 1998);

"public postal licensee's installation or plant" means any installation or plant used for postal purposes belonging to or used by the public postal licensee;

"radio communication" means the emitting or receiving over paths which are not provided by any material substance constructed or arranged for that purpose, of electro-magnetic energy of a frequency not exceeding three million megahertz being energy which either—

(i) is capable of being transmitted through a telecommunication system; or

(ii) is used in connection with the determination of position, bearing or distance, or for the gaining of information as to the presence, absence or, motion of any object or objects of any class;

"radio communication apparatus" means any apparatus capable of being used or adapted for radio communication and where the context so requires, includes a radio communication station;

"radio communication station" means any telecommunication station capable of being used or being adapted for radio communication;

"registration agent" means a person contracted or otherwise engaged by a telecommunications operator to carry out registration of SIM-cards;

"repository" means a system for storing and retrieving certificates or other information relevant to certificates;

"signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;

"signature-creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

"signature-creation device" means configured software or hardware used to implement the signature-creation data;

"significant market power" means a position of economic strength enjoyed by a licensee which enables it to prevent effective competition being maintained on the relevant market by affording it the power to behave independently of its competitors, customers and consumers;

"SIM-card"means the Subscriber Identity Module which is an independent electronically-activated device designed for use in conjunction with a telecommunication apparatus to enable the user of the telecommunication apparatus to transmit and receive indirect communications by providing access to telecommunication systems and enabling such telecommunication systems to identify the particular Subscriber Identity Module and its installed information;

"subscription management service" means a service which consists of the provision of support services to a subscription broadcasting service which support services may include, but not limited to, subscriber management support, subscription fee collection, call centres, sales and marketing, and technical and installation support;

"telecommunication apparatus" means apparatus constructed or adapted for use in transmitting anything which is transmissible by a telecommunication system or in conveying anything which is transmitted through such a system;

"telecommunication line" means any wire, cable, tube, pipe or other similar thing which is designed or adapted for use in connection with the operation of a telecommunication system or a radio communication apparatus with any casing, coating, tube or pipe enclosing the same and any appliances and apparatus connected therewith for the same; and includes any structure, post or other thing in, by or from which any telecommunication and radio-communication apparatus is or may be installed, supported, carried or suspended;

"telecommunication officer" means any person employed either permanently or temporarily by a telecommunication operator in connection with a telecommunication system licensed under section 79;

"telecommunication operator" means a telecommunication operator licensed under section 79;

"telecommunication service" means any of the following—

(i) a service consisting of the conveyance by means of a telecommunication system of anything falling within subparagraphs (i) to (v) in the definition of "telecommunication system";

(ii) a service consisting of the installation, maintenance, adjustment, repair, alteration, moving, removal or replacement of apparatus which is or is to be connected to a telecommunication system; or

(iii)a directory information service, being a service consisting of the provision by means of a telecommunication system of directory information for the purposes of facilitating the use of a service

falling within subparagraph (i) above and provided by means of that system;

"telecommunication system" means a system for the conveyance, through the agency of electric, magnetic, electro-magnetic, electro-chemical or electro-mechanical energy, of—

(i) speech, music and other sounds;

(ii) visual images;

(iii) data;

(iv) signals serving for the impartation (whether as between persons and persons, things and things or persons and things) of any matter otherwise than in the form of sound, visual images or data; or

(v) signals serving for the activation or control of machinery or apparatus and includes any cable for the distribution of anything falling within (i) to (iv) above;

"Tribunal" means the Appeals Tribunal set up under section 102 of this Act;

"vandalize" means to commit an act of vandalism;

"vessel" includes any ship, boat, air-cushioned vehicle or floating rig or platform used in navigation.

(2) For the purpose of this Act, a telecommunication system is operated by the person who controls and manages it by himself or through servants or agents.

(3) In this Act—

(a) a postal article shall be deemed to have been delivered—

(i) to the addressee, if it is delivered into the private letter box of the addressee, leaving it at the house, or office of the addressee as set out thereon, or with his employee or agent or other persons authorised to receive it and, where the addressee is a guest or is resident at a hotel, hostel or lodgings, it is left with the proprietor or manager thereof or with his agent; or

(ii) to a postal services operator licensed under section 51, if it is deposited into a posting box or handed over to an employee or agent of a postal services operator authorised to receive it;

(b) a postal article shall be deemed to be in the course of transmission by post from the time of its being delivered to the

public postal licensee until the time of its being delivered to the addressee, or it is returned to the sender or otherwise disposed of under the provisions of this Act;

(c) save as otherwise agreed to between the originator and the addressee—

(i) the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator;

(ii) if the addressee has a designated computer resource for the purpose of receiving an electronic record, receipt occurs at the time when the electronic record enters the designated computer resource; or

(iii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee; or

(iv) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee;

(v) an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business; and

(vi) the provisions of subparagraph (v) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under subparagraphs (ii) or (iii). [Act No. 1 of 2009, s. 4, Act No. 12 of 2012, Sch, Act No. 41A of 2013, s. 2(1), Act No. 25 of 2015, Sch.]

PART VIA—ELECTRONIC TRANSACTIONS AND CYBER SECURITY

83B. Application

(1) This Part shall not apply to any rule or law requiring writing or signatures in any of the following matters—

(a) the creation or execution of a will;

(b) negotiable instruments;

(c) documents of title.

(2) The Minister may by order modify the provisions of subsection (1) by adding or removing any class of transactions or matters.

83C. Functions of the Commission in relation to electronic transactions and cyber security

(1) The functions of the Commission in relation to electronic transactions shall be to—

(a) facilitate electronic transactions and cyber security by ensuring the use of reliable electronic records;

(b) facilitate electronic commerce and eliminate barriers to electronic commerce such as those resulting from uncertainties over writing and signature requirements;

(c) promote public confidence in the integrity and reliability of electronic records and electronic transactions and cyber security;

(d) foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium;

(e) promote and facilitate efficient delivery of public sector services by means of reliable electronic records;

(f) develop sound frameworks to minimize the incidence of forged electronic records and fraud in electronic commerce and other electronic transactions and cyber security;

(g) promote and facilitate the efficient management of critical internet resources; and

(h) develop a framework for facilitating the investigation and prosecution of cybercrime offences.

(2) The Cabinet Secretary, in consultation with the Authority may make regulations with respect to cyber security.

[Act No. 1 of 2009, s. 31, Act No. 41A of 2013, s. 24, Act No. 25 of 2015, Sch.]

83D. Requirement for a licence

(1) No person shall—

(a) operate an electronic certification system; or

(b) update a repository or administer a sub-domain in the Kenya country top level domain (.ke ccTLD), except in accordance with a licence granted under this Act.

(2) A person who contravenes this section commits an offence and shall be liable on conviction to a fine not exceeding three hundred thousand shillings or to imprisonment for a term not exceeding three years, or both.

[Act No. 1 of 2009, s. 31.]

83E. Licence for electronic certification services

(1) The Commission may, upon application in a prescribed manner and subject to such conditions as it may deem necessary, grant licences under this section authorizing a person to provide electronic certification services.

(2) A licence granted under subsection (1) may require a licensee to—

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to procedures that ensure that the secrecy and privacy of the electronic signatures are assured; and

(d) observe such other standards as may be specified by regulations.

[Act No. 1 of 2009, s. 31.]

83F. Licence for country code top-level domain

The Commission may, upon application in the prescribed manner and subject to such conditions as it may deem necessary, grant licences under this section authorizing a person to administer a sub-domain in the country code top-level domain.

[Act No. 1 of 2009, s. 31.]

83G. Legal recognition of electronic records

Where any law provides that information or other matter shall be in writing then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

[Act No. 1 of 2009, s. 31.]

83H. Retention of electronic records

Where any law provides that documents, records or information shall be retained for any specific period, then that requirement shall be deemed to have been satisfied where such documents, records or information are retained in electronic form if—

(a) the information contained therein remains accessible so as to be usable for subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; and

(c) the details which will facilitate the identification of the original destination, date and time of dispatch or receipt of such electronic record are available in the electronic record;

Provided that this clause shall not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

[Act No. 1 of 2009, s. 31.]

83I. Retention of information in original form

(1) Where any law requires information to be presented or retained in its original form, that requirement is met by an electronic record if—

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form as an electronic message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Subsection (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subsection (1)(a) —

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in light of all the relevant circumstances.

[Act No. 1 of 2009, s. 31.]

83J. Formation and validity of contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and acceptance of an offer may be expressed by means of electronic messages thus where an electronic message is used in the formation of a contract, the contract shall not be denied validity or enforceability solely on the ground that an electronic message was used for the purpose.

(2) Nothing in this section shall apply to any law that expressly provides a different method for the formation of a valid contract.

[Act No. 1 of 2009, s. 31.]

83K. Recognition of parties of electronic messages

As between the originator and the addressee of an electronic message, a declaration of intent or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic message.

[Act No. 1 of 2009, s. 31.]

83L. Attribution of electronic records

(1) An electronic message shall be attributed to the originator if it was sent by the originator himself, or by a person who had the authority to act on behalf of the originator in respect of the electronic record or by an information system programmed by or on behalf of the originator to operate automatically.

(2) As between an originator and an addressee, an addressee is entitled to regard an electronic message as being that of the originator, and act on that assumption, if—

(a) in order to ascertain whether the electronic message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for the purpose; or

(b) the electronic message as received by addressee resulted from actions of a person who had the authority to act on behalf of the originator in respect of the electronic record.

[Act No. 1 of 2009, s. 31.]

83M. Acknowledgement of receipt

(1) Where the originator has not agreed with the addressee that the acknowledgement of receipt of electronic records be given in a particular form or by a particular method, an acknowledgement may be given by—

(a) any communication by the addressee, automated or otherwise;

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that an electronic record shall be binding only on receipt of an acknowledgement of such electronic record, then, unless acknowledgement has been received, the electronic record shall be deemed to have never been sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding on receipt of such acknowledgement, and acknowledgement has not been received by the originator within a reasonable time, then, the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement must be received by him and if no acknowledgement is received within that time limit, he may, after giving notice to the addressee, treat the electronic record as though it was never sent.

[Act No. 1 of 2009, s. 31.]

83N. Secure electronic record

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from that point of time to verification.

[Act No. 1 of 2009, s. 31.]

83O. Compliance with requirement for a signature

(1) Where any law requires a signature of a person, that requirement is met in relation to an electronic message if an advanced electronic signature is used that is as reliable as was appropriate for the purpose for which the electronic message was generated or communicated, in light of all the circumstances, including any relevant agreement.

(2) Subsection (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An advanced electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in subsection (1) if—

(a) it is generated through a signature-creation device;

(b) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(c) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(d) any alteration to the electronic signature made after the time of signing is detectable; and

(e) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing, is detectable.

[Act No. 1 of 2009, s. 31.]

83P. Legal recognition of electronic signatures

Where any law provides that information or any other matter shall be authenticated by affixing a signature or that any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in that law, such requirement shall be deemed to have been satisfied if such information is authenticated by means of an advanced electronic signature affixed in such manner as may be prescribed by the Minister.

[Act No. 1 of 2009, s. 31.]

83Q. Protected systems

(1) The Minister may, by notification in the *Gazette*, declare that any computer system or computer network is a protected system.

(2) The Minister may, by order in writing, authorize any person to access protected systems notified under subsection (1).

(3) Any person who secures unauthorized access or attempts to secure unauthorized access to a protected system commits an offence and is liable on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term of ten years or to both.

[Act No. 1 of 2009, s. 31, Act No. 41A of 2013, s. 25.]

83R. Regulations for electronic signatures

The Minister may, in consultation with the Commission, for the purposes of this Act, prescribe regulations on—

(a) the type of electronic signature;

(b) the manner and format in which the electronic signature shall be affixed;

(c) the manner and procedure which facilitates identification of the person affixing the electronic signature;

(d) control of the processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to electronic signatures.

[Act No. 1 of 2009, s. 31.]

83S. Use of electronic records and electronic signatures in Government and its agencies

(1) Where any law provides for—

(a) the effective delivery of public goods and services, improving quality of life for disadvantaged communities, strengthening good governance and public participation, creation of a better business environment, improving productivity and efficiency of government departments;

(b) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the Government in a particular manner;

(c) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner; or

(d) the receipt or payment of money in a particular manner, then notwithstanding anything contained in such law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic forms as may be prescribed by the Minister in consultation with the Commission.

(2) The Minister may, for the purposes of subsection (1), by regulations prescribe—

(a) the manner and format in which such electronic records shall be filed, created or used;

(b) the manner or method of payment of any fee or charges for filing, creation or issue of any electronic record under subparagraph (a).

[Act No. 1 of 2009, s. 31.]

83T. Electronic *Gazette*

Where any law provides that any rule, regulation, order, notification, or any other matter shall be published in the *Gazette*, then such requirement shall be deemed to have been satisfied if such rule, regulation, order, notification or any other matter is published in the electronic *Gazette*;

Provided that where any rule, regulation, order, by-law, notification or any other matter is published both in the printed and electronic *Gazettes*, the date of publication shall be deemed to be the date of the *Gazette* which was first published in any form.

[Act No. 1 of 2009, s. 31.]

83U. Alteration, deletion, suppression etc., of telecommunication system

Any person who intentionally and without authorization, engages in the input, acquisition, alteration, deletion or suppression of a telecommunication system or otherwise alters the authenticity or integrity of such a system, with the intent that it be considered or acted upon for legal purposes as though it were authentic or with integrity, regardless of whether or not the system is directly readable or intelligible, for any unlawful purpose, commits an offence and shall be liable, on conviction, to a fine not exceeding five million shillings or to imprisonment for a term of not exceeding five years or to both.

[Act No. 1 of 2009, s. 31, Act No. 41A of 2013, s. 26.]

83V. Regulations

The Cabinet Secretary, in consultation with the Authority may make regulations under this Part.

[Act No. 1 of 2009, s. 31, Act No. 41A of 2013, s. 27, Act No. 25 of 2015, Sch.]

83W. Unauthorized access to and interception of computer service

(1) Subject to subsection (3), any person who by any means knowingly—

(a) secures access to any computer system for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within a computer system, shall commit an offence.

(2) A person convicted for an offence under subsection (1) shall be liable on conviction to a fine not exceeding five hundred thousand shillings or to imprisonment for a term not exceeding three years or both.

(3) Where as a result of the commission of an offence under subsection (1), the operation of the computer system, is impaired, or data contained in the computer system is suppressed or modified, the person convicted of such offence shall be liable on conviction to a fine not exceeding two hundred thousand shillings or to imprisonment for a term not exceeding two years or both.

(4) For the purpose of this section, it is immaterial that the unauthorized access or interception is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

(5) A person shall not be liable under subsection (1) where he—

(a) has the express or implied consent of both the person who sent the data and the intended recipient of such data;

(b) is acting in reliance of any statutory power.

[Act No. 1 of 2009, s. 31.]

continued on page K9–62

83X.Unauthorized modification of computer material

(1) Subject to subsections (3) and (4), any person who, knowingly does an act which causes an unauthorized modification of data held in any computer system shall, on conviction be liable to a fine not exceeding five hundred thousand shillings or imprisonment for a term not exceeding three years or both.

(2) Where as a result of the commission of an offence under this section—

(a) the operation of the computer system;

(b) access to any program or data held in any computer; or

(c) the operation of any program or the reliability of any data, is suppressed, modified or otherwise impaired,

a person convicted for the offence shall be liable on conviction to a fine not exceeding two hundred thousand shillings and or imprisonment for a term not exceeding two years or both.

(3) A person shall not be liable under this section where he is acting in reliance of any statutory power.

(4) A modification is unauthorized if—

(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

(b) he does not have consent to the modification from any person who is so entitled.

(5) For the purposes of this section, it is immaterial whether an unauthorized modification or any intended effect of it, be permanent or merely temporary.

[Act No. 1 of 2009, s. 31.]

83Y. Damaging or denying access to computer system

Any person who without lawful authority or lawful excuse does an act which causes directly or indirectly—

(a) a degradation, failure, interruption or obstruction of the operation of a computer system; or

(b) a denial of access to, or impairment of any program or data stored in, the computer system, shall commit an offence and shall, on conviction be liable to a fine not exceeding two hundred thousand shillings and or imprisonment for a term not exceeding two years or both.

[Act No. 1 of 2009, s. 31.]

83Z. Unauthorized disclosure of password

Any person who knowingly discloses any password, access code, or any other means of gaining access to any program or data held in any computer system—

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that the disclosure is likely to cause prejudice to any person,

shall commit an offence and shall, on conviction, be liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

[Act No. 1 of 2009, s. 31.]

84A. Unlawful possession of devices and data

(1) Any person who knowingly manufactures, sells, procures for use, imports, distributes or otherwise makes available a computer system or any other device designed or adapted primarily for the purpose of committing any offence under sections 83U to 83Z, shall commit an offence.

(2) Any person who knowingly receives, or is in possession, without sufficient excuse or justification, of one or more of the devices under subsection (1) shall commit an offence.

(3) Any person who is found in possession of any data or program with the intention that the data or program be used, by the person himself or another person, to commit or facilitate the commission of an offence under this Act, shall commit an offence.

(4) For the purposes of subsection (3), possession of any data or program includes—

(a) having possession of a computer system or data storage device that holds or contains the data or program;

(b) having possession of a document in which the data or program is recorded; or

(c) having control of data or program that is in the possession of another person.(5) Where a person is convicted under this section, he shall on conviction be liable to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

[Act No. 1 of 2009, s. 31.]

84B. Electronic fraud

Any person who fraudulently causes loss of property to another person by—

(a) any input, alteration, deletion or suppression of data; or

(b) any interference with the functioning of a computer system,

with intent to procure for himself or another person, an advantage, shall commit an offence and shall, on conviction be liable to a fine not exceeding two hundred thousand shillings and or imprisonment for a term not exceeding three years or both.

[Act No. 1 of 2009, s. 31.]

84C. Tampering with computer source documents

Any person who knowingly or intentionally conceals, destroys or alters, or intentionally or knowingly causes another person to conceal, destroy or alter any computer source code, computer programme, computer system or computer network, where the computer source code is required to be kept or maintained by law for the time being in force, shall on conviction be liable to a fine not exceeding three hundred thousand shillings or imprisonment for a term not exceeding three years, or both.

[Act No. 1 of 2009, s. 31.]

84D. Publishing of obscene information in electronic form

Any person who publishes or transmits or causes to be published in electronic form, any material which is lascivious or appeals to the prurient interest and its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied therein, shall on conviction be liable to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or both.

[Act No. 1 of 2009, s. 31.]

84E. Publication for fraudulent purpose

Any person who knowingly creates, publishes or otherwise makes available an electronic signature certificate for any fraudulent or unlawful purpose commits an offence and shall on conviction be liable to a fine not exceeding one million shillings or imprisonment for a term not exceeding five years, or both.

[Act No. 1 of 2009, s. 31.]

84F. Unauthorized access to protected systems

Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this Part shall be guilty of an offence and shall on conviction be liable to a fine not exceeding one million shillings or imprisonment for a term not exceeding five years, or both.

[Act No. 1 of 2009, s. 31.]

84G. Re-programming of mobile telephone

(1) Any person who knowingly or intentionally, not being a manufacturer of mobile telephone devices or authorized agent of such manufacturer, changes mobile telephone equipment identity, or interferes

with the operation of the mobile telephone equipment identity, commits an offence.

(2) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding one million shillings or to imprisonment for a term not exceeding five years or both.

[Act No. 1 of 2009, s. 31.]

84H. Possession or supply of anything for re-programming mobile telephone

(1) A person commits an offence if he—

(a) has in his custody or under his control anything which may be used for the purpose of changing or interfering with the operation of a mobile telephone equipment identifier; and

(b) intends to use the thing unlawfully for that purpose or to allow it to be used unlawfully for that purpose; or

(c) supplies anything which may be used for the purpose of changing or interfering with the operation of a mobile telephone equipment; and

(d) knows or believes that the person to whom the thing is supplied intends to use it unlawfully for that purpose or to allow it to be used unlawfully for that purpose; or

(e) offers to supply anything which may be used for the purpose of changing or interfering with the operation of a mobile telephone equipment identifier; and

(f)knows or believes that the person to whom the thing is offered intends if it is supplied to him to use it unlawfully for that purpose or to allow it to be used unlawfully for that purpose.

(2) A person guilty of an offence under this section is liable on conviction to a fine not exceeding one million shillings or to imprisonment for a term not exceeding five years or to both.

[Act No. 1 of 2009, s. 31.]

84I. *Bonafide* re-programming or possession

It shall not be an offence under sections 84G and 84H if—

(a) the re-programming of mobile telephone equipment identity is done; or

(b) the possession of anything that can change the mobile telephone equipment identity is had,

bonafides for personal technological pursuits or other technological review endeavours.

[Act No. 1 of 2009, s. 31.]

PART VIB – UNIVERSAL SERVICE FUND

84J. Establishment of the Fund

(1) There is hereby established a fund to be known as the Universal Service Fund which shall be managed and administered by the Commission.

(2) The object a nd the purpose of the Fund shall be to support widespread access to, support capacity building and promote innovation in information and communications technology services.

(3) There shall be a universal service levy (in this Part referred to as the "levy") that shall be charged by the Commission on the licensees under this Act for purposes of the Universal Service Fund.

[Act No. 1 of 2009, s. 31.]

84K. Revenue and expenditure of the Fund

(1) There shall be credited to the Fund—

(a) levies from licensees;

(b) such monies as may be provided by Parliament for that purpose;

(c) *deleted by Act No. 41A of 2013, s. 28* ;

(d) income from any investment made by the Fund; and

(e) any gifts, donations, grants and endowments made to the Fund.

(2) There shall be paid out of the Fund any expenditure approved by the Board for the purposes of and the administration of the Fund.

[Act No. 1 of 2009, s. 31, Act No. 41A of 2013, s. 28.]

84L. *Repealed by Act No. 41A of 2013, s. 29* .

[Act No. 1 of 2009, s. 31, Act No. 41A of 2013, s. 29]

84M. *Repealed by Act No. 41A of 2013, s. 29* .

[Act No. 1 of 2009, s. 31, Act No. 41A of 2013, s. 29.]

84N. *Repealed by Act No. 41A of 2013, s. 29* .

[Act No. 1 of 2009, s. 31, Act No. 41A of 2013, s. 29.]

84O. Fund's annual returns and audit

The Board shall comply with the Public Audit Act as regards the operations of the Fund.

[Act No. 1 of 2009, s. 31.]

84P. Regulations with respect to the Fund

The Minister may, in consultation with the Commission, make regulations generally with respect to the administration of the Fund and without prejudice to the generality of the foregoing, with respect to—

(a) amount of levy;

(b) operations of the Fund;

(c) mechanisms for accessing the Fund;

(d) mechanisms for collection of the levy; or

(e) prescribing anything that may be prescribed under this Part.